Abstract algebra Exam 1

Question 1

Let $a = 4901$ and $b = 3432$.

Using the Euclidean algorithm, find the greatest common divisor (a, b) of a and b and express (a, b) as a linear combination of a and b with integer coefficients.

Use your results to factor a and b as products of primes.

We have:

$$c = a - b = 4901 - 3432 = 1469,$$
$$d = b - 2c = 3432 - 2938 = 494,$$
$$e = c - 2d = 1469 - 988 = 481,$$
$$f = d - e = 494 - 481 = 13,$$
$$g = e - 37f = 481 - 481 = 0.$$

So the last non-zero remainder, namely f is the greatest common divisor, so we have $(a, b) = 13$.

Then we have:

$f = d-e = d-(c-2d) = 3d-c = 3(b-2c)-c = 3b-7c = 3b-7(a-b) = 10b-7a.$

Check: $10b - 7a = 34320 - 34307 = 13$.
Dividing a by 13, we get:

$$\frac{a}{13} = \frac{4901}{13} = 377.$$

We see that 377 has a factor of 13: $377 = 390 - 13 = 13(30 - 1) = 13(29)$.

So $a = 13(13)(29)$ expresses a as a product of primes.

Dividing b by 13, we get:

$$\frac{b}{13} = \frac{3432}{13} = 264 = 2(132) = 2(2)(66) = 2(2)(2)(33) = 2(2)(2)(3)(11).$$

So $b = 2(2)(2)(3)(11)(13)$ expresses b as a product of primes.

Question 2

Let $a(x) = x^4 + 2x^3 - 7x^2 - 20x - 12$ and $b(x) = x^3 + 4x^2 + 7x + 6$.

Using the Euclidean algorithm, find the greatest common divisor $(a(x), b(x))$ of $a(x)$ and $b(x)$ and express $(a(x), b(x))$ as a linear combination of $a(x)$ and $b(x)$ with polynomial coefficients.

Use your results to factor $a(x)$ and $b(x)$ as products of irreducibles.

We have:

$$c = a-(x-2)b = x^4+2x^3-7x^2-20x-12-(x^4+4x^3+7x^2+6x)+2x^3+8x^2+14x+12$$
$$= -6x^2 - 12x.$$

Then we have:

$$d = b + \left(\frac{x+2}{6}\right) c = x^3 + 4x^2 + 7x + 6 - x^3 - 2x^2 - 2x^2 - 4x = 3x + 6.$$

Finally we have:

$$e = c + 2xd = -6x^2 - 12x + 6x^2 + 12x = 0.$$

Since d is the last non-zero remainder the required g.cd. is the monic polynomial proportional to d, so is:

$$(a, b) = \frac{d}{3} = x + 2.$$

Then we have:

$$(a, b) = \frac{d}{3} = \frac{1}{3}\left(b + \left(\frac{x+2}{6}\right) c\right)$$
$$= \frac{b}{3} + \left(\frac{x+2}{18}\right) c = \frac{b}{3} + \left(\frac{x+2}{18}\right) (a - (x-2)b)$$
$$= \left(\frac{x+2}{18}\right) a + \frac{b}{18}(6 - (x-2)(x+2))$$
$$= \left(\frac{x+2}{18}\right) a + \left(\frac{10 - x^2}{18}\right) b.$$

This expresses (a, b) as a linear combination of a and b with polynomial coefficients, as required.

To factor b, we see that b has (a, b) as a factor, so factoring, we get:

$$b = x^3 + 4x^2 + 7x + 6 = (x + 2)(x^2 + 2x + 3).$$

Now the discriminant of the quadratic $x^2 + 2x + 3$ is:

$$2^2 - 4(1)(3) = 4 - 12 = -8 < 0.$$

So the quadratic $x^2 + 2x + 3$ has no real roots, so is irreducible over the reals. We can also see this by completing the square:

$$x^2 + 2x + 3 = x^2 + 2x + 1 + 2 = (x + 1)^2 + 2.$$

So $b = (x + 2)(x^2 + 2x + 3)$ expresses b as a product of irreducibles.

Similarly, factoring a, we get:

$$a = x^4 + 2x^3 - 7x^2 - 20x - 12 = (x + 2)(x^3 - 7x - 6).$$

Now the polynomial $g(x) = x^3 - 7x - 6$ vanishes at $x = -1$, since we have:

$$g(-1) = (-1)^3 - 7(-1) - 6 = -1 + 7 - 6 = 0.$$

So $g(x)$ has a factor of $x + 1$.
Factoring, we get:

$$g(x) = x^3 - 7x - 6 = (x + 1)(x^2 - x - 6) = (x + 1)(x + 2)(x - 3).$$

So $a = (x - 3)(x + 1)(x + 2)(x + 2)$, expresses a as a product of irreducibles and we are done.

Question 3

For each of the following equations, determine with proof if it is solvable and for each solvable equation find all integer solutions; if an equation is not solvable prove that it is not solvable:

- $45x = 599 \mod 49$.
  The numbers 45 and 49 are co-prime, so we get, working mod 49.
  $$x = \frac{599}{45} = \frac{599+49}{45-49} = \frac{648}{-4} = -162 = -162 + 4(49) = 34.$$
  So the general solution is $x = 34 + 49k$, with k any integer.

- $1001x = 52 \mod 39$.
  We need integers x and y such that:
  $$1001x + 39y = 52.$$
  Each term has a factor of 13, so we divide and get:
  $$77x + 3y = 4.$$
  Since $(77, 3)$ this is solvable and x is unique mod 3.
  Working mod 3, we need:
  $$77x = 4,$$
  $$(77 - 3(25))x = 4,$$
  $$2x = 4,$$
  $$x = 2.$$
  So the general solution is $x = 2 + 3q$, with q any integer.

- $x^2 - 6x - 1 = 0 \mod 17$.
  We complete the square:
  $$x^2 - 6x = 1, \quad x^2 - 6x + 9 = 10, \quad (x-3)^2 = 10.$$
  Now we compute all the squares mod 17:
  $$0^2 = 0, \quad (\pm 1)^2 = 1, \quad (\pm 2)^2 = 4, \quad (\pm 3)^2 = 9, \quad (\pm 4)^2 = 16,$$
  $$(\pm 5)^2 = 25 = 25 - 17 = 8, \quad (\pm 6)^2 = 36 = 36 - 2(17) = 2,$$
  $$(\pm 7)^2 = 49 = 49 - 2(17) = 15, \quad (\pm 8)^2 = 64 = 64 - 3(17) = 13.$$
  So 10 is not a square mod 17, so the given equation has no solutions.

Question 4

- Find all integer solutions x of the following system:

$$55x = 49 \mod 19$$
$$4x = 3 \mod 11$$

- Also find the number of integer solutions of the system with $|x| < 10000$.

We can use the Chinese Remainder Theorem, since 19 and 11 are co-prime.

- The first subsidiary problem is:

$$55x_1 = 49 \mod 19$$
$$4x_1 = 0 \mod 11$$

The second equation is solved by $x_1 = 11p$ for some integer p, since 4 is invertible mod 11.

Then, working mod 19, the first equation becomes:

$$55(11p) = 49,$$
$$(55 - 3(19))(11p) = 49 - 3(19),$$
$$-2(11p) = -8,$$
$$p = \frac{8}{22} = \frac{4}{11} = \frac{4}{11-19} = \frac{4}{-8} = -\frac{1}{2} = -\frac{1+19}{2} = -10 = 19-10 = 9.$$

So we get $x_1 = 11(9) = 99 \mod (11)(19) = 99 \mod 209$.

- The second subsidiary problem is:

$$55x_2 = 0 \mod 19$$
$$4x_2 = 3 \mod 11$$

The first equation is solved by $x_2 = 19q$ for some integer q, since 55 is invertible mod 19.

Then, working mod 11, the second equation becomes:

$$4(19q) = 3,$$

$$76q = 3,$$

$$(76 - 7(11))q = 3,$$

$$-q = 3,$$

$$q = -3 = 11 - 3 = 8.$$

So we get $x_2 = 19(8) = 152 \mod 209$.

So the required problem is solved by $x = x_1 + x_2 = 99 + 152 = 251 \mod 209 = 251 - 209 = 42 \mod 209$.
So the general integral solution is $x = 42 + 209k$, where k is any integer.
For the last part, we need:

$$-10000 < 42 + 209k < 10000,$$

$$-10042 < 209k < 9958$$
$$-\frac{10042}{209} < k < \frac{9958}{209}.$$

Now we have: $48(209) = (50 - 2)209 = 10450 - 418 = 10032$.
So $-49(209) < -10042 < -48(209)$ and $47(209) < 9958 < 48(209)$.
So we get, since k is an integer:

$$-48 \leq k \leq 47,$$

$$1 \leq k + 49 \leq 96.$$

So there are exactly 96 solutions x to the system with $|x| < 10000$.

Question 5

For each of the following either give an example, with proof, or explain why no such example can exist:

- A ring $\mathbb{A}$ with exactly four distinct units.

  Since $\mathbb{Z}_5$ is a field, since 5 is prime, all four of its non-zero elements are units, so $\mathbb{A} = \mathbb{Z}_5$ will do (since the fifth element of $\mathbb{Z}_5$, namely 0, is not a unit).

- A ring $\mathbb{B}$ with exactly six elements, which has a non-trivial subring (i.e. a subring with at least two elements, that is not the whole of $\mathbb{B}$).

  The ring $\mathbb{B}$ of all even numbers mod 12 will do: $\mathbb{B} = \{0, 2, 4, 6, 8, 10\}$ mod 12, since it is easily seen to be closed under multiplication and subtraction in $\mathbb{Z}_{12}$ so is a subring and has six elements.
  Then the subset of $\mathbb{B}$, $\mathbb{C} = \{0, 4, 8\}$ mod 12 is also closed under multiplication and subtraction in $\mathbb{Z}_{12}$, so is a non-trivial subring of $\mathbb{B}$, as required.

- A field $\mathbb{F}$ such that $\mathbb{F} \times \mathbb{F}$ is also a field.

  In $\mathbb{F} \times \mathbb{F}$ we have the formula $(1, 0)(0, 1) = (0, 0)$, where 1 is the identity of $\mathbb{F}$, so $\mathbb{F} \times \mathbb{F}$ has divisors of zero, so cannot be a field.

- A subring $\mathbb{S}$ of the ring of two by two real matrices, such that the product of any two elements of $\mathbb{S}$ is zero and yet $\mathbb{S}$ has an infinite number of elements.

  The following set $\mathbb{S}$ will do:

  $$\mathbb{S} = \left\{ M_x = \begin{vmatrix} 0 & x \\ 0 & 0 \end{vmatrix} \text{ for each } x \in \mathbb{R} \right\}.$$

  It is easily checked that $M_x - M_y = M_{x-y}$ and $M_x M_y = 0 = M_0$, for any x and y in $\mathbb{R}$, so $\mathbb{S}$ is closed under subtraction and multiplication, so is a subring of $\mathbb{M}_{2\times 2}(\mathbb{R})$, with trivial multiplication, as required.
  Also $\mathbb{S}$ has an uncountable infinity of elements, since $\mathbb{S}$ is in one-to-one correspondence with $\mathbb{R}$ itself, so we are done.

Question 6

Find, with proof, all solutions of the equation $x^2 = x \mod 12$.
Hence or otherwise, find all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}_{12}$ and for each such homomorphism, identify its kernel and image.

We compute all squares mod 12:

$$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 = 4, 5^2 = 25 = 1, 6^2 = 36 = 0,$$

$$7^2 = 49 = 1, 8^2 = 64 = 4, 9^2 = 81 = 9, 10^2 = 100 = 4, 11^2 = 121 = 1.$$

So, by inspection, the only solutions of the equation $x^2 = x \mod 12$ are $x = 0, 1, 4, 9 \mod 12$.

For a ring homomorphism f from $\mathbb{Z}$ to $\mathbb{Z}_{12}$, if $f(1) = a$, then $f(n) = na$.
For this to be a homomorphism, since the map is clearly linear, we need just $f(mn) = f(m)f(n)$, for all m and n, so $a(mn) = (am)(an) = a^2(mn)$.
Putting $m = n = 1$, we need $a^2 = a$ and then f is a homomorphism, as required.
So there are precisely four homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}_{12}$:

- The trivial homomorphism, $f_0 : n \to 0 \mod 12$, for all $n \in \mathbb{Z}$.
  The image of f_0 is $\{0\}$.
  The kernel of f_0 is $\mathbb{Z}$.

- The identity homomorphism, $f_1 : n \to n \mod 12$, for all $n \in \mathbb{Z}$.
  The image of f_1 is $\mathbb{Z}_{12}$.
  The kernel of f_1 is the set of all integer multiples of 12.

- The homomorphism, $f_4 : n \to 4n \mod 12$, for all $n \in \mathbb{Z}$.
  The image of f_4 is $\{0, 4, 8\} \mod 12$.
  The kernel of f_4 is the set of all integer multiples of 3.

- The homomorphism, $f_9 : n \to 9n \mod 12$, for all $n \in \mathbb{Z}$.
  The image of f_9 is $\{0, 3, 6, 9\} \mod 12$.
  The kernel of f_9 is the set of all integer multiples of 4.

Question 7

Let $\mathbb{A} = \mathbb{Z}_4 \times \mathbb{Z}_6$, $\mathbb{B} = \mathbb{Z}_3 \times \mathbb{Z}_8$ and $\mathbb{C} = \mathbb{Z}_{24}$.
Decide, with proof, which of the rings $\mathbb{A}$, $\mathbb{B}$, or $\mathbb{C}$ are isomorphic to each other.

- For an isomorphism of rings with identity, the identity must go to the identity.
  So for an isomorphism of $\mathbb{Z}_{24}$ with $\mathbb{Z}_4 \times \mathbb{Z}_6$, the map must be $x \to (x, x)$.
  But then $12 \to (12, 12) = (0, 0)$, so 12 is in the kernel of the map, so the map is not one-to-one, so is not in fact an isomorphism.
  So $\mathbb{C}$ and $\mathbb{A}$ are not isomorphic.

- On the other hand the homomorphism $x \to (x, x)$ from $\mathbb{C}$ to $\mathbb{B}$ maps x to zero if and only if $x = 0 \mod 3$ and $x = 0 \mod 8$.
  By the Chinese Remainder Theorem this implies that $x = 0 \mod 24$, so $x = 0$ in $\mathbb{C}$.
  So the kernel is zero, so the map is one-to-one.
  Then, since the two rings both have 24 elements, the map must be onto also, by the pigeonhole principle.
  So the map is an isomorphism.
  So $\mathbb{B}$ and $\mathbb{C}$ are isomorphic.

- Finally if $\mathbb{A}$ and $\mathbb{B}$ were isomorphic, then the composition of that isomorphism with the known isomorphism of $\mathbb{B}$ with $\mathbb{C}$ would give an isomorphism of $\mathbb{A}$ and $\mathbb{C}$, which does not exist.
  So $\mathbb{A}$ and $\mathbb{B}$ cannot be isomorphic and we are done.